Crittografia su Curve Ellittiche

Crittografia

Luciano Margara

Unibo

2022

Campo

Un campo K è un insieme non vuoto dotato di due operazioni che soddisfano le proprietà associativa, commutativa, di esistenza dell'elemento neutro e di esistenza dell'inverso di ciascun elemento (ad eccezione dello zero per la moltiplicazione)

Notazione

$(K, +, *)$ è un campo (field) se e solo se

$(K, +)$ è un gruppo abeliano con elemento neutro 0

$(K \setminus \{0\}, *)$ è un gruppo abeliano con elemento neutro 1

Moltiplicazione distributiva rispetto all'addizione:
$\forall a, b, c \in G : \ a * (b + c) = (a * b) + (a * c)$

Notazione

$(\mathbb{Q}, +, *)$ è un campo con le operazioni classiche di somma e prodotto

$(\mathbb{R}, +, *)$ è un campo con le operazioni classiche di somma e prodotto

$(\mathbb{C}, +, *)$ è un campo con le operazioni classiche di somma e prodotto

$(\mathbb{Z}_p, +, *)$ è un campo con le operazioni di somma e prodotto modulo p primo

$(\mathbb{Z}, +, *)$ non è un campo con le operazioni di somma e prodotto perché gli unici elementi invertibili per la moltiplicazioni sono 1 e -1

L'insieme degli interi Z non è un campo perché, per definizione, in un campo ogni elemento diverso da zero deve avere un inverso moltiplicativo, ovvero, per ogni 'a' appartenente a Z con a!=0, deve esistere un a^−1 appartenente a Z tale che: a*a^−1 = 1

Caratteristica

La caratteristica di un campo K è un modo per misurare quante volte bisogna sommare l'unità moltiplicativa 1 a sé stessa affinché il risultato sia lo zero, che è l'elemento neutro rispetto all'addizione.

La caratteristica di un campo è definita come il più piccolo numero naturale k tale che sommando k volte l'elemento neutro moltiplicativo del campo K (indicato con 1), si ottiene l'elemento neutro additivo di K (indicato con 0). Se un tale k non esiste, la caratteristica è 0 per definizione

Pensa alla caratteristica come al "ciclo" che si compie sommandosi continuamente l'unità. Se dopo un certo numero di somme ritorni al punto di partenza (cioè ottieni lo zero additivo), questo numero di somme è la caratteristica. Se, invece, sommare ripetutamente 1 non porta mai allo zero, allora il campo non ha un ciclo "chiuso" e si dice che la caratteristica è 0.

Caratteristica

La caratteristica di $(\mathbb{Q}, +, *)$ è 0 perchè non ha cicli

La caratteristica di $(\mathbb{Z}_p, +, *)$ è p in quanto

$$\overbrace{1 + \cdots + 1}^{p \text{ volte}} = 0$$

Infatti, ha cicli

Curva Ellittica

Nella sua forma più generale, una curva ellittica E su un campo K è definita come l'insieme dei punti $(x, y) \in K^2$ che soddisfano l'equazione algebrica

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

dove $a, b, c, d, e \in K$

Forma normale di Weierstrass

Se la caratteristica del campo K è diversa da 2 e da 3, l'equazione che definisce una curva ellittica si può ridurre all'equazione cubica in forma normale di Weierstrass

$$y^2 = x^3 + ax + b$$

Somma su Curve Ellittiche

La peculiarità che rende le curve ellittiche utilizzabili nelle applicazioni crittografiche è la possibilità di attribuire, all'insieme dei punti di una curva, la struttura algebrica di un gruppo abeliano additivo, ovvero di definire una legge di composizione interna che permette di associare ad ogni coppia di punti sulla curva, un terzo punto sempre sulla curva.

Dati due punti P e Q sulla curva, si traccia la retta che li congiunge. Questa retta interseca la curva in un terzo punto, che indichiamo come R. Poi, si riflette R rispetto all'asse x (ossia, si cambia il segno della coordinata y) ottenendo il punto P+Q.

L'insieme dei punti (x,y) che soddisfano questa equazione (della curva ellittica), insieme a un punto speciale chiamato "punto all'infinito" (che funge da elemento neutro), forma un insieme su cui possiamo definire una legge di composizione interna.

Somma su Curve Ellittiche

La legge di composizione (addizione o somma su curve ellittiche), è associativa, commutativa, ammette un elemento neutro (tale cioè che la somma di questo elemento con un punto della curva è uguale al punto stesso) ed è tale che sia definito l'inverso di ogni punto, come richiesto dalla definizione di gruppo abeliano. Una curva ellittica su K è quindi l'insieme dei punti $(x, y) \in K^2$ che soddisfano l'equazione $y^2 = x^3 + ax + b$, oltre al punto neutro.

Curve Ellittiche sui Reali

Assumiamo per il momento che la curva sia definita nel campo $\mathbb{R}$ dei numeri reali e che sia dunque rappresentabile nel piano cartesiano. L'elemento neutro O sarà il punto all'infinito sull'asse delle ordinate. La curva sarà costituita dall'insieme $E(a, b)$ dei punti $(x, y) \in \mathbb{R}^2$ che soddisfano l'equazione $y^2 = x^3 + ax + b$, notando che essa contiene il punto all'infinito O ovvero:

$$E(a, b) = \{(x, y) \in \mathbb{R}^2 : \ y^2 = x^3 + ax + b\}$$

Punto all'Infinito

La forma standard della curva ellittica fa sì che tutte le rette, indipendentemente dalla direzione con cui vengono prolungate, convergano in un unico punto all'infinito.

O è il punto all'infinito in direzione dell'asse y. Rette parallele si incontrano all'infinito nello stesso punto, che è unico indipendentemente dalla direzione in cui le rette sono percorse.

si intende che l'insieme dei punti all'infinito si riduce a un solo punto (l'elemento neutro del gruppo definito sulla curva) e quindi, anche se in un piano proiettivo generico le rette parallele di direzioni diverse si incontrano in punti diversi, nella rappresentazione standard della curva ellittica si assume (o si dimostra) che esiste un solo punto all'infinito, che si identifica (per convenzione) come quello in direzione dell'asse y.

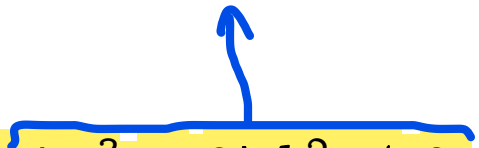
In altre parole, se si "somma" (mediante la legge geometrica) un punto P della curva con O, si ottiene P.

Punto all'Infinito

Per $x \to \infty$, l'equazione $y^2 = x^3 + ax + b$ tende alla $y^2 = x^3$, ovvero $y = \pm x^{3/2}$, con derivata $y' = \pm \frac{3}{2} x^{1/2}$. Quindi per $x \to \infty$ si ha $y' \to \pm\infty$, ovvero la curva contiene quindi il punto O

Curve Ellittiche sui Reali

La condizione che viene richiesta affinché la curva sia priva di singolarità è che il discriminante non sia nullo

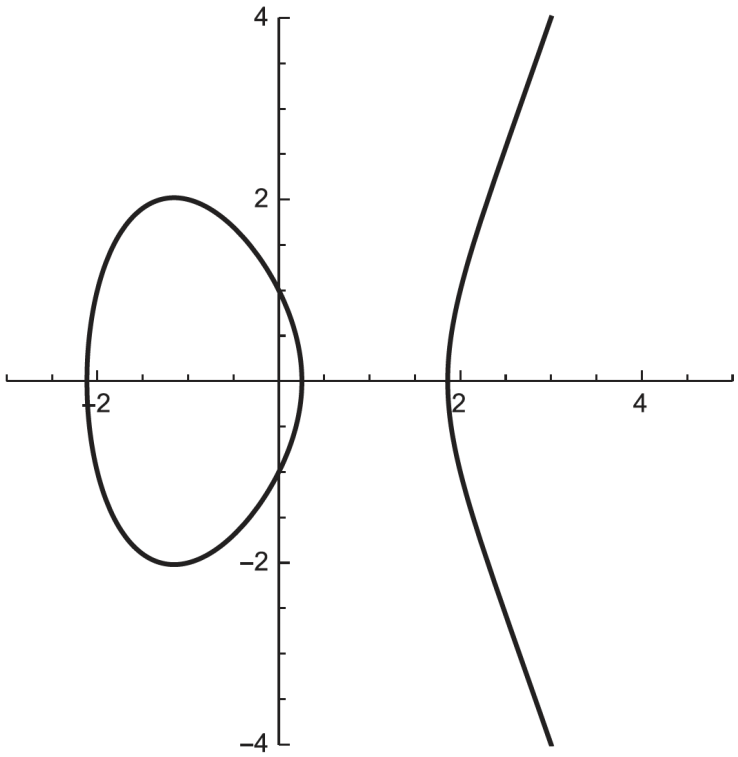


Assumiamo inoltre che sia $4a^3 + 27b^2 \neq 0$: questa condizione assicura che il polinomio cubico $x^3 + ax + b$ non abbia radici multiple e che di conseguenza la curva sia priva di punti singolari come cuspidi o nodi dove non sarebbe definita in modo univoco la tangente

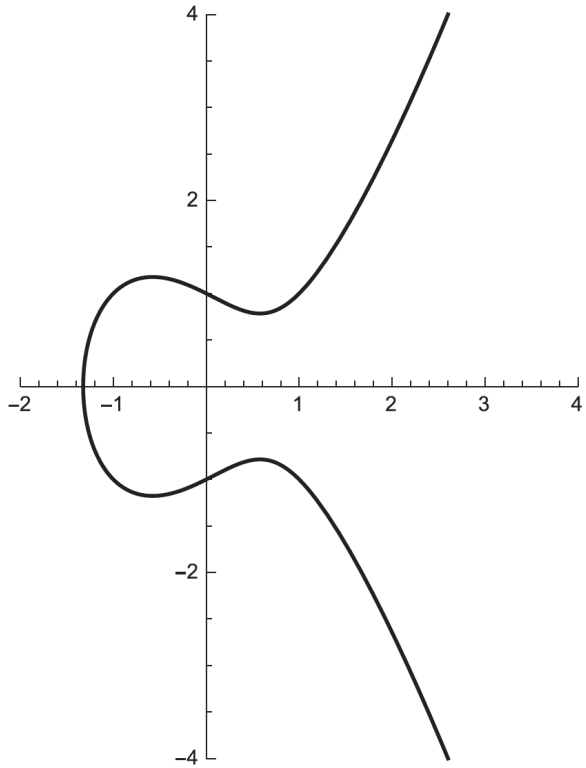
Esempi di curve ellittiche sui Reali

discriminante = −16(4a^3+27b^2)

In entrambi i casi, nessuna delle due curve presenta punti singolari.



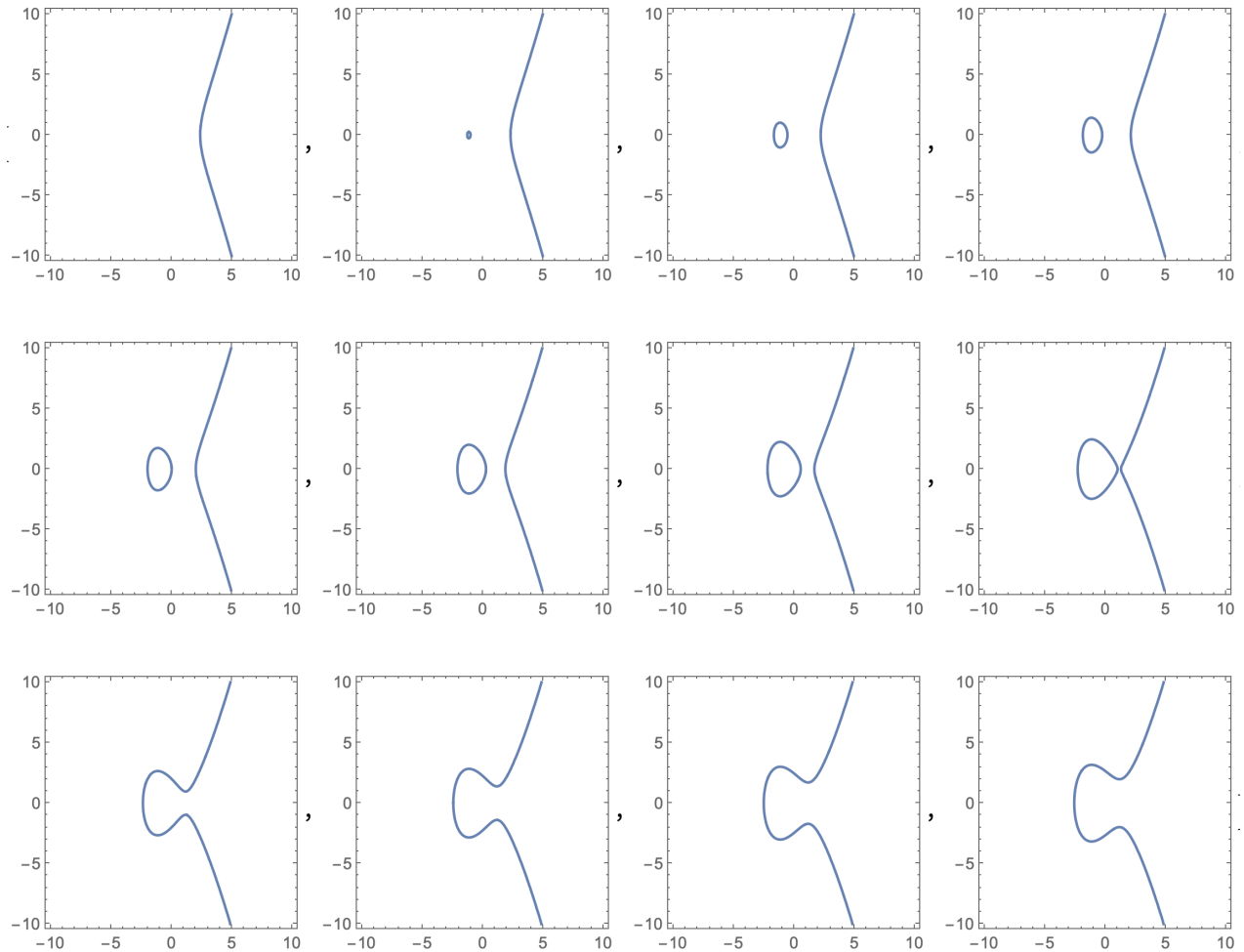
(a) Curva $y^2 = x^3 - 4x + 1$



(b) Curva $y^2 = x^3 - x + 1$

Due componenti separate se il polinomio cubico x^3+ax+b ha tre radici reali. In questo caso, una di queste componenti è un “ovale” chiuso, mentre l’altra si estende all’infinito. Una sola componente se il polinomio ha una sola radice reale (le altre due sono complesse coniugate). In questo caso, la curva reale è un’unica linea “a S” (o simile) che si estende indefinitamente.

$$y^2 = x^3 - 4x + e \text{ con } e = -4, -3, \ldots, 6, 7$$



Curve Ellittiche sui Reali: proprietà

Il grafico delle curve ellittiche sui reali può assumere una tra due possibili forme: una forma a due componenti che si presenta quando il polinomio in x ha tre radici reali, e una forma con una sola componente che si presenta quando il polinomio ha una sola radice reale. In entrambi i casi, le curve ellittiche presentano una simmetria orizzontale: ogni punto $P = (x, y)$ sulla curva si riflette rispetto all'asse delle ascisse nel punto $(x, -y)$ anch'esso sulla curva, che indicheremo con $-P$ (l'immagine speculare rispetto all'asse x del punto all'infinito O è lo stesso O).

cioè rispetto all'asse x

Se un punto P=(x,y) sta sulla curva, allora anche (x,−y) appartiene alla curva.

Intersezione Curve Ellittiche sui Reali e rette

Ogni retta interseca una curva ellittica in ~~al più~~ tre punti. al massimo

Intersezione Curve Ellittiche sui Reali e rette

Infatti intersecando una curva di terzo grado con una di primo grado (retta) e sostituendo nella prima l'espressione di y della seconda, si ottiene un'equazione di terzo grado in x che ha tre soluzioni, reali o complesse, corrispondenti alle ascisse dei punti di intersezione tra la curva ellittica e la retta.

Intersezione Curve Ellittiche sui Reali e rette

Nel piano proiettivo (dove le curve ellittiche sono naturalmente considerate), ogni retta e ogni curva cubica si intersecano in tre punti se si contano correttamente le intersezioni. Nel piano reale, però, può capitare di “vedere” soltanto una o due intersezioni reali, mentre le altre avvengono:

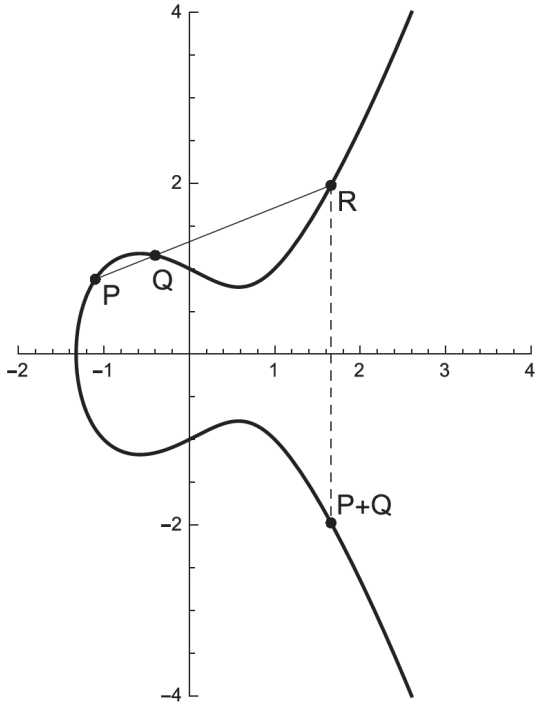
- O in punti complessi (che si presentano a coppie di coniugati complessi);
- O in un punto all’infinito (che può anche avere molteplicità maggiore di 1).

Possiamo quindi avere una soluzione reale e due soluzioni complesse e coniugate, quindi un punto (reale) di intersezione (intersezione della curva con una retta orizzontale di ordinata sufficientemente elevata o con una retta verticale che incontri la curva solo nel punto all’infinito).

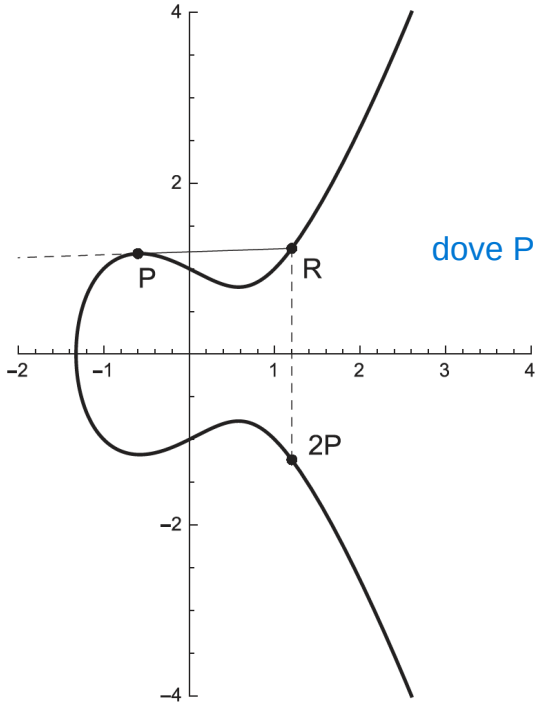
Intersezione Curve Ellittiche sui Reali e rette

Oppure si hanno tre soluzioni reali, quindi tre punti di intersezione. Quindi se una retta interseca la curva $E(a, b)$ in due punti P e Q, coincidenti se la retta è una tangente, allora la retta interseca $E(a, b)$ anche in un terzo punto R. In particolare se la retta è verticale, essa interseca la curva $E(a, b)$ nei due punti P e Q (in questo caso $Q = -P$) e nel punto all'infinito O.

Esempi di curve ellittiche sui Reali



(a) Somma di due punti P e Q.



(b) Raddoppio di un punto P

dove P e R stessa y

Addizione su Curve Ellittiche

La definizione dell'operazione di addizione su una curva ellittica è basata sulle proprietà appena enunciate. Dati tre punti P, Q, R di una curva ellittica $E(a, b)$, se P, Q e R sono disposti su una retta, allora la loro somma si pone uguale al punto all'infinito:

$$P + Q + R = O$$

Da questa definizione, è possibile ricavare la regola per sommare due punti P e Q.

Addizione su Curve Ellittiche

- Si considera la retta passante per P e Q, oppure l'unica tangente alla curva in P nel caso P e Q coincidano.
- Si determina il punto di intersezione R tra la curva e la retta per P e Q, oppure tra la curva e la tangente in P per $P = Q$.
- Si definisce somma di P e Q il punto simmetrico a R rispetto all'asse delle ascisse, ovvero si pone $P + Q = -R$.

Addizione su Curve Ellittiche

P e Q distinti e $P \neq -Q$
$P = (x_P, y_P)$, $Q = (x_Q, y_Q)$,
$P + Q = S = (x_S, y_S)$

$\lambda = (y_Q - y_P)/(x_Q - x_P)$
λ è il coefficiente angolare della retta che passa per P e Q

$x_S = \lambda^2 - x_P - x_Q$
$y_S = -y_P + \lambda(x_P - x_S)$

Addizione su Curve Ellittiche

$P = Q$
$P = (x_P, y_P)$, $2P = S = (x_S, y_S)$

$y_p \neq 0 \implies \lambda = (3x_P^2 + a)/(2y_P)$ λ è il coefficiente angolare della retta tangente P

$y_p = 0 \implies$ tangente verticale $\implies 2P = 0$

Addizione su Curve Ellittiche

La somma è ben definita in quanto, come abbiamo già osservato, anche $-R$ è un punto della curva. Nel caso particolare in cui P e Q abbiano la stessa coordinata x, ovvero se $Q = -P$, i due punti sono allineati lungo una verticale che interseca la curva nel punto all'infinito e si pone $P + Q = P + (-P) = O$, in quanto il simmetrico di O rispetto all'asse delle ascisse è sempre O. Questa legge di addizione attribuisce all'insieme dei punti di una curva ellittica $E(a, b)$ la struttura algebrica di un gruppo abeliano additivo, che ha per elemento neutro il punto all'infinito O.

Addizione su Curve Ellittiche

- Chiusura: $\forall P, Q \in E(a, b) : P + Q \in E(a, b)$
- Elemento neutro:
  $\forall P \in E(a, b) : P + O = O + P = P$ (infatti le rette passanti per O sono verticali, dunque la retta per P e O interseca la curva in $-P$, il cui simmetrico è P)
- Assiociatività:
  $\forall P, Q, R \in E(a, b) : P + (Q + R) = (P + Q) + R$
- Commutatività: $\forall P, Q \in E(a, b) : P + Q = Q + P$

Curve Ellittiche su un Campo Finito

Passiamo ora ad esaminare le curve ellittiche definite sui campi finiti, le uniche di interesse per la crittografia. Gli algoritmi crittografici hanno infatti bisogno di un'aritmetica veloce e precisa e pertanto non possono utilizzare le curve ellittiche sui reali che richiedono elaborazioni lente e inaccurate a causa degli errori di arrotondamento. Inoltre potremo lavorare in aritmetica modulare ove, come abbiamo già visto, alcuni problemi divengono computazionalmente difficili

Curve Ellittiche su $\mathbb{Z}_p$

Utilizziamo l'insieme $\mathbb{Z}_p$ degli interi modulo un numero primo p. Nel campo $\mathbb{Z}_p$ tutte le operazioni si intendono in algebra modulare, e dunque coinvolgono interi compresi fra 0 e $p-1$. La caratteristica del campo è p, per cui ci limiteremo a considerare campi $\mathbb{Z}_p$ con $p > 3$ in modo da poter ridurre l'equazione generale di una curva ellittica alla forma normale di Weierstrass. Le curve ellittiche con variabili e coefficienti ristretti agli elementi del campo $\mathbb{Z}_p$ sono chiamate curve ellittiche prime

Curve Ellittiche su $\mathbb{Z}_p$

Presi dunque $a, b \in \mathbb{Z}_p$, la curva ellittica prima $E_p(a, b)$ è definita come l'insieme dei punti che soddisfano l'equazione $y^2 = x^3 + ax + b$ modulo p insieme al punto all'infinito (elemento neutro)

$$E_p(a, b) =$$

$$\{(x, y) \in \mathbb{Z}^2 : \ y^2 \ mod \ p = (x^3 + ax + b) \ mod \ p\} \cup \{O\}$$

Esempi di curve ellittiche su $\mathbb{Z}_p$

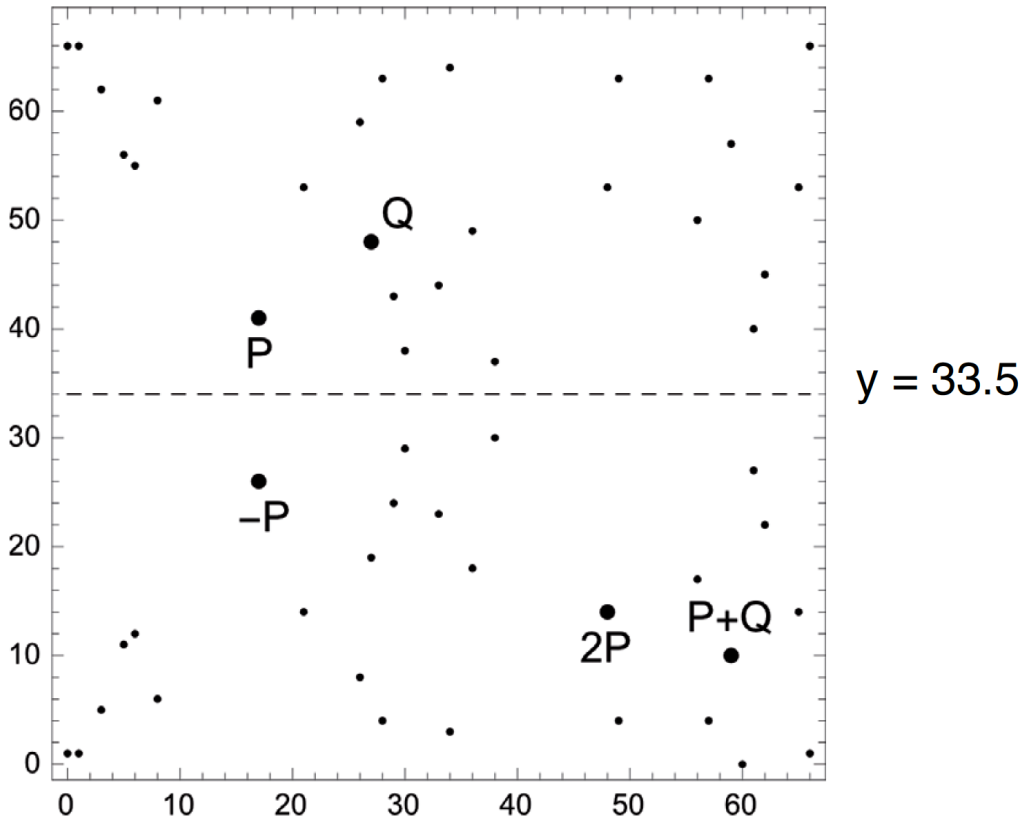


Figura 8.4: La curva ellittica prima $E_{67}(-1, 1)$.

Curve Ellittiche su $\mathbb{Z}_p$

Si può dimostrare che se il polinomio

$$x^3 + ax + b \ mod \ p$$

non ha radici multiple, ovvero se

$$4a^3 + 27b^2 \ mod \ p \neq 0$$

i punti della curva prima $E_p(a, b)$ formano un gruppo abeliano finito rispetto all'operazione di addizione

Curve Ellittiche su $\mathbb{Z}_p$

Data la natura discreta delle curve prime non è più possibile descrivere questa operazione in termini geometrici, tuttavia le regole e la formulazione algebrica della somma definite per le curve ellittiche sui numeri reali si possono immediatamente adattare al caso finito, con l'unica accortezza di intendere ed eseguire tutte le operazioni in algebra modulare

Curve Ellittiche su $\mathbb{Z}_p$

Eseguendo questi calcoli per i punti

$$P = (17, 41) \text{ e } Q = (27, 48)$$

si ottengono i punti

$$P + Q = (59, 10) \text{ e } 2P = (48, 14)$$

Controlliamo che $(59, 10)$ appartenga alla curva:

$$y^2 \ mod \ p = 10^2 \ mod \ 67 = 33$$

$$x^3 - x + 1 \ mod \ p = 59^3 - 59 + 1 \ mod \ 67 = 33$$

Curve Ellittiche su $\mathbb{Z}_p$: ordine

Un parametro importante ai fini della sicurezza delle applicazioni crittografiche basate sulle curve ellittiche è l'ordine di una curva, ovvero il suo numero di punti. Una curva prima $E_p(a, b)$ può avere al più $2p + 1$ punti: il punto all'infinito e le p coppie di punti (x, y) e $(x, -y)$ che soddisfano l'equazione $y^2 = x^3 + ax + b$ in modulo, al variare di x in $\mathbb{Z}_p$.

Curve Ellittiche su $\mathbb{Z}_p$: ordine

Purtroppo non esistono limiti inferiori per il numero di punti di $E_p(a, b)$.
Ci si può comunque aspettare che la curva contenga $\Theta(p)$ punti considerando che i residui quadratici di $\mathbb{Z}_p$, cioè gli elementi del campo che ammettono radice quadrata in $\mathbb{Z}_p$, sono esattamente $(p-1)/2$

Curve Ellittiche binarie

Oltre alle curve prime, la crittografia su curve ellittiche utilizza un'altra famiglia di curve ellittiche, chiamate curve ellittiche binarie. Si tratta delle curve i cui coefficienti e le cui variabili assumono valore nel campo $GF(2^m)$, costituito da 2^m elementi che si possono pensare come tutti gli interi binari di m cifre e su cui si può operare mediante l'aritmetica polinomiale modulare.

Logaritmo Discreto

Per definire un sistema crittografico a chiave pubblica usando le curve ellittiche occorre per prima cosa individuare una buona funzione one-way con trap-door che ne garantisca la sicurezza. RSA e il protocollo di Diffie e Hellman per lo scambio delle chiavi sono basati rispettivamente sul problema della fattorizzazione e sul problema del logaritmo discreto nell'algebra modulare.

Logaritmo Discreto

Per le curve ellittiche si può definire una funzione one-way con trap-door analoga al logaritmo discreto nell'algebra modulare. In effetti, l'operazione di addizione di punti di una curva ellittica su un campo finito presenta delle analogie con l'operazione di prodotto modulare.

Logaritmo Discreto

Fissato un intero positivo k possiamo mettere in relazione l'elevamento alla potenza k di un intero in modulo con la moltiplicazione scalare per k di un punto P di una curva ellittica, operazione che consiste nel sommare P con se stesso k volte.
Entrambe le operazioni si possono eseguire in tempo polinomiale

Logaritmo Discreto

L'esponenziazione modulare e la moltiplicazione scalare su una curva ellittica hanno dunque una struttura molto simile, pur con le diverse notazioni (moltiplicativa e additiva) utilizzate: la prima operazione si riferisce al processo di moltiplicazione di x per se stesso k volte, mentre la seconda al processo di addizione di P con se stesso k volte.

Logaritmo Discreto

Consideriamo ora l'operazione inversa della moltiplicazione scalare su una curva ellittica, ovvero dati due punti P e Q trovare, se esiste, il più piccolo intero k tale che $Q = kP$. Questo problema è noto come il problema del logaritmo discreto per le curve ellittiche, in analogia al problema del logaritmo discreto su insiemi finiti, operazione inversa dell'esponenziazione modulare. Il numero intero k, quando definito, è chiamato logaritmo in base P del punto Q.

Logaritmo Discreto

Il problema del logaritmo discreto per le curve ellittiche risulta computazionalmente difficile perché tutti gli algoritmi noti per risolverlo hanno complessità esponenziale.
Il Metodo a forza bruta basato sul calcolo di tutti i multipli di P fino a trovare Q, è chiaramente improponibile se k è sufficientemente grande

Logaritmo Discreto

Abbiamo così individuato una funzione computazionalmente trattabile in una direzione (calcolo di $Q = kP$ dati P e k), ma praticamente intrattabile nell'altra (calcolo di k dati P e $Q = kP$), vale a dire una funzione one-way con trap door su cui basare la sicurezza della crittografia su curve ellittiche.

Scambio Chiavi su Curve Ellittiche

- Alice e Bob si accordano pubblicamente su un campo finito e su una curva ellittica definita su questo campo. Quindi scelgono, nella curva, un punto B di ordine n molto grande, ove l'ordine n di un punto è il più piccolo intero positivo n tale che $nB = O$
- Alice sceglie un intero positivo casuale $n_A < n$ come propria chiave privata, genera una chiave pubblica $P_A = n_A B$ e la spedisce in chiaro a Bob. La chiave pubblica corrisponde dunque ad un punto della curva scelto casualmente

Scambio Chiavi su Curve Ellittiche

- Bob sceglie un intero positivo casuale $n_B < n$ come propria chiave privata, genera una chiave pubblica $P_B = n_B B$ e la spedisce in chiaro a Alice. Di nuovo, la chiave pubblica è un punto della curva scelto casualmente
- Alice riceve P_B e calcola $n_A P_B = n_A n_B B = S$ usando la sua chiave privata n_A (si noti che S è un punto della curva)
- Bob riceve P_A e calcola $n_B P_A = n_B n_A B = S$ usando la sua chiave privata n_B

Scambio Chiavi su Curve Ellittiche

- A questo punto Alice e Bob condividono lo stesso punto S determinato dalle scelte casuali di entrambi. Per trasformare S in una chiave segreta k per la cifratura simmetrica convenzionale occorre convertirlo in un numero intero. Ad esempio si pone

$$k = x_S \ mod \ 2^{256}$$

ovvero k è costituito dagli ultimi 256 bit dell'ascissa di S

Scambio Chiavi su Curve Ellittiche

Un crittoanalista che ha intercettato i messaggi P_A e P_B scambiati in chiaro tra i due partner e che conosce i parametri della curva ellittica impiegata e il punto B, non è in grado di violare lo schema in quanto per calcolare S dovrebbe calcolare n_A dati B e P_A, oppure n_B dati B e P_B, ovvero dovrebbe risolvere il problema del logaritmo discreto per le curve ellittiche, certamente intrattabile in questo caso date le dimensioni dei valori coinvolti. Il protocollo è comunque vulnerabile agli attacchi attivi di tipo man-in-the-middle, esattamente come il protocollo DH sui campi finiti.

Scambio di Messaggi su Curve Ellittiche: Idea di base

Per cifrare un messaggio m codificato come numero intero utilizzando le curve ellittiche occorre per prima cosa trasformare m in un punto di una curva ellittica, che sarà a sua volta trasformato in un nuovo punto da usare come testo cifrato

Scambio di Messaggi su Curve Ellittiche: Idea di base

Non si tratta di un compito semplice e infatti non è noto alcun algoritmo deterministico polinomiale per effettuare una tale trasformazione. Esistono tuttavia degli algoritmi randomizzati molto efficienti che hanno una probabilità arbitrariamente bassa di fallire, cioè di non produrre un punto della curva

Algoritmo di Koblitz

Supponiamo di voler trasformare un numero intero positivo $m < p$ in un punto di una curva ellittica prima $E_p(a, b)$. Usando m come ascissa, la probabilità di trovare un punto della curva è pari alla probabilità che $m^3 + am + b \ mod \ p$ sia un residuo quadratico che sappiamo essere dalla teoria circa $1/2$

Algoritmo di Koblitz

- Fissiamo un intero positivo h tale che $(m+1)h < p$
- Consideriamo gli interi $x = mh + i$, al variare di i da 0 a $h-1$
- Per ciascun x si prova ad estrarre la radice quadrata y di $x^3 + ax + b \ mod \ p$, operazione polinomiale se p è primo
- Se la radice esiste ritorniamo il punto $P_m = (x, y)$
- Iteriamo la procedura fino a quando si trova una radice, oppure i raggiunge il valore h e concludiamo che non è stato possibile trasformare il messaggio in un punto della curva

Algoritmo di Koblitz: Esempio

- $y^2 = x^3 - 4x + 1$
- $p = 7919$, $h = 10$, $m = 12$
- $(12 + 1)10 < 7919$
- $120^3 - 4 \cdot 120 + 1 \mod 7919$ non è un residuo quadratico
- $121^3 - 4 \cdot 121 + 1 \mod 7919$ non è un residuo quadratico
- $122^3 - 4 \cdot 122 + 1 \mod 7919$ è un residuo quadratico !
- $3411^2 \mod 7919 = 1910$
- $122^3 - 4 \cdot 122 + 1 \mod 7919 = 1910$
- Codifica di 12: $(12, 3411)$

Algoritmo di Koblitz

Benché la distribuzione delle ascisse dei punti della curva non segua una legge nota, ci si può aspettare che la probabilità che, per ogni valore di x considerato, $x^3 + ax + b$ non sia un quadrato modulo p sia circa $1/2$. Quindi il metodo ha una probabilità di fallire pari a circa 2^{-h}

Dal messaggio al punto

Per risalire al messaggio dal punto $P_m = (x, y)$ individuato basta calcolare

$$m = \lfloor x/h \rfloor$$

si noti in proposito che è stato scelto $(m+1)h < p$ per evitare che il messaggio sia corrotto dalle operazioni in modulo

Codifica

Mittente e Destinatario si accordano pubblicamente

- su una specifica curva ellittica
- su un punto B della curva che abbia ordine n elevato
- su un intero h per la trasformazione dei messaggi in punti della curva

Generazione delle chiavi

Ogni utente D genera la propria coppia chiave pubblica e chiave privata scegliendo un intero casuale $n_D < n$ come chiave privata e pubblicando la chiave $P_D = n_D B$

Abbiamo usato la lettera D invece che U (utente) per enfatizzare il ruolo di destinatario

Codifica

Il Mittente

- Trasforma il messaggio m nel punto P_m sulla curva
- Sceglie un intero casuale r e calcola i due punti $V = rB$ e $W = P_m + rP_D$ dove P_D è la chiave pubblica del Destinatario
- Invia al Destinatario $\langle V, W \rangle$

Decodifica

- Il destinatario conosce n_D che è la sua chiave privata
- Il destinatario riceve $V = rB$
- Cosa è $n_D\, V$?
- $n_D\, V = n_D rB = r n_D\, B$
- Cosa è rP_D?
- $rP_D = r n_D\, B$
- Quindi $n_D\, V = rP_D$

Decodifica

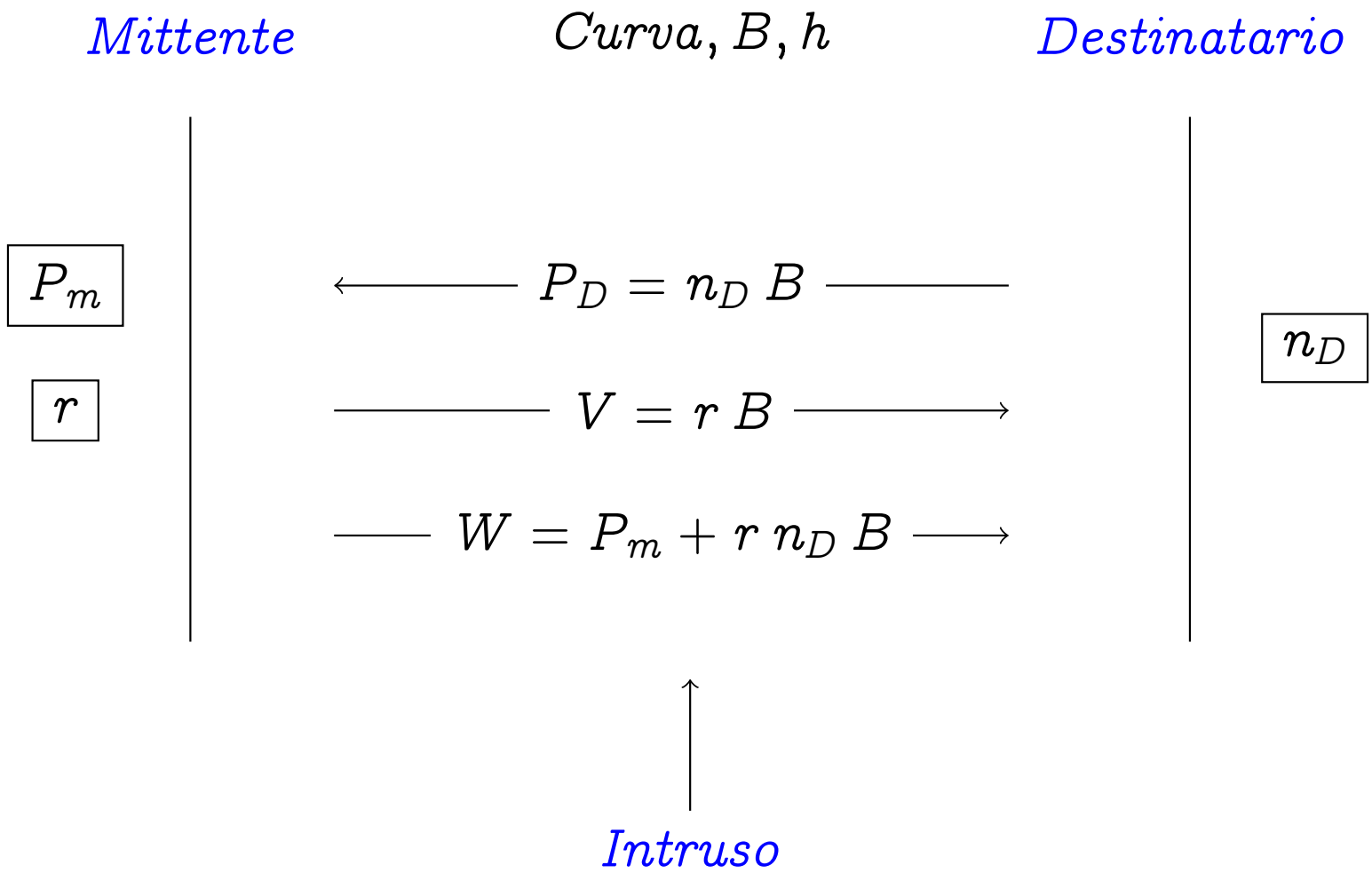
Il Desinatario

- Riceve $\langle V, W \rangle$ dal Mittente
- Ricostruisce il punto P_m con la sua chiave privata n_D, calcolando

$$\begin{aligned} W - n_D V &= P_m + rP_D - n_D(rB) \\ P_D = n_D B \implies &= P_m + r(n_D B) - n_D(rB) \\ &= P_m \end{aligned}$$

- Trasforma P_m nel messaggio m

ECC


Mittente
Curva, B, h
Destinatario
P_m
r
$P_D = n_D\, B$
$V = r\, B$
$W = P_m + r\, n_D\, B$
n_D
Intruso

Sicurezza

La sicurezza della crittografia su curve ellittiche è strettamente legata alla difficoltà di calcolare il logaritmo discreto di un punto, ovvero di calcolare l'intero k dati P e $Q = kP$, problema per cui ad oggi non è noto alcun algoritmo efficiente di risoluzione

Sicurezza e lunghezza delle chiavi

TDEA, AES (bit della chiave)	*RSA* e *DH* (bit del modulo)	*ECC* (bit dell'ordine)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Misura universale di sicurezza

L'idea è di misurare la quantità di energia necessaria per forzare il sistema e confrontarla con la quantità di acqua che quell'energia potrebbe far bollire.
Usando questa misura si può verificare che forzare un cifrario RSA a 228 bit richiede meno energia di quella necessaria per far bollire un cucchiaino di acqua.
L'energia necessaria per forzare un sistema basato su curve ellittiche a 228 bit potrebbe far bollire tutta l'acqua sulla Terra.